QKD Reference List

Hao Chung

last revised: January 24, 2018

There are two reviews for general issues of QKD. The first one [SBPC+09] is written by Lutkenhaus *et al.* and the second one [ABB+14] is written by Renner *et al.* , so both ones are reliable.

1 Lo's Paradigm

The first unconditional security proof was given by Mayers [May96], but it is complicated. Then, Lo and Chau [LC99] gave a security proof for entanglement-distillation protocol (EDP) and Shor and Preskill [SP00] showed that EDP is equivalent to BB84. The chapter 12. of [NC00] gives a nice introduction to SP00 proof.

Later, Inamori-Lutkenhaus-Mayers [ILM07] and Gottesman-Lo-Lutkenhaus-Preskill [GLLP04] gave a proof for more general case. While I have not read [ILM07], both of them are called "standard security proof" in Lo's paper [LCQ12] so I think ILM has the similar importance as GLLP in QKD.

2 Renner's Paradigm

Renner [Ren05] first gave the security definition in terms of trace distance. Tomamichel and Leverrier [TL17] gave a self-contained proof for EDP and BB84 in Renner's paradigm.

Tomamichel [TL17] says that "Koashi [Koa06] first brought to light that security can be certified using an entropic form of Heisenberg's uncertainty principle." However, in the suggested list of prof. Ma, he suggests reading [Koa09].

The operational meaning of min-entropy and max-entropy is surveyed by Konig, Renner, and Schaffner [KRS09].

3 Device Independence

Fully device independence. The idea of device independence was introduced by Mayers and Yao [MY98]. Vazirani and Vidick [VV14] gave a proof for fully device independence.

Decoy. The idea of decoy was introduced by Hwang [Hwa03]. Later, Lo, Ma and Chen [LMC05] gave a security proof for decoy protocol and the precise parameters of their protocol are analyzed in [MQZL05].

MDI. The first protocol and security proof for measurement device independent (MDI) QKD was given by [LCQ12]. Later, Lo [XCQL15] gave a survey paper for MDI QKD which also introduced some attack for QKD that can be protected by MDI QKD. It is worth noting that the main idea of the proof of MDI is the "time-reversed EDP," which is proposed by [BHM96].

4 Quantum Hacking

Photon number splitting (PNS) attack. By the statements in [LJ02], this kind of attack was first mentioned in [HIGM95]. However, [LJ02] is a better introduction to PNS attack.

Faked states attack. The idea of faked states attack is proposed by Makarov and Hjelme [MH05]. They define this kind of attack as follow:

Definition 1 (Faked states attack)**.** *Faked states attack on a quantum cryptosystem is an intercept-and-re- send attack where Eve does not try to reconstruct the original states, but generates instead light pulses that get detected by the legitimate parties in a way controlled by her while not setting off any alarms.*

In particular, there are two kinds of specific faked states attack.

- **Time-shift attack.** Lo [XCQL15] reported that the first successful quantum hacking against a commercial QKD system is the "time-shift attack." The idea of the time-shift attack was proposed in [QFLM07] and implemented in [ZFQ+08].
- **Detector blinding attack.** The other more powerful attack is "detector blinding attack, which is introduced in [LWW+10]. In the same paper, they also showed that this attack can break a commercial QKD system.

  For more references about time-shift attack and detector blinding attack, we can check the citations in [XCQL15].

Trojan horse attack. The idea of Trojan horse attack was mentioned by Lo [Lo01]. The idea is that the signals sent by Alice may not live in a two-dimentional space so that they may convey additional information (e.g. the bases Alice uses) for Eve to probe.

There are some methods to create such "Trojan horse" for Eve.

- **Large pulse attack.** Eve can send optic pulses to Alice's or Bob's apparatus and measure the reflective pulses. If the pulses are reflected by the modulator in Alice's or Bob's apparatus, Eve can know the bases they use without causing any error [VMH01].

5 Differential Phase Shift QKD

Differential phase shift (DPS). The idea and the first DPS QKD protocol was proposed by Inoue, Waks and Yamamoto [IWY02]. The security proof under the assumption of single-photon source was given in [WTY09]. Later, Koashi *et al.* [TKK12] gave a security proof of "coherent-state-based" DPS, which can resist photon number splitting attack. Note that Koashi also gave an explicit EDP version of RRDPS in [TKK12].

Round-robin differential phase shift (RRDPS). In 2014, Sasaki, Yamamoto and Koashi [SYK14] proposed the first RRDPS protocol, which is the first QKD protocol that decouples the signal disturbance and the parameter of privacy amplification as claimed by [TSTK15]. Later, Takesue *et al.* first demostrated the experiment of RRDPS QKD [TSTK15].

In [SYK14], the authors claim that they have shown the security of RRDPS, while we have not fully understood it.

Sasaki and Koashi [SK17] gave another security proof of RRDPS QKD based on the signal disturbance, that is, the traditional Shor-Preskill (EDP) argument.

Besides, I also find other people give a security proof of RRDPS QKD [LS17].

6 Experiment

Decoy. In laboratory, the decoy protocol is performed by a signal generator at gigahertz which achieves the key rate of 1.02 Mbit/s for a fiber distance of 20 km and 10.1 kbit/s for 100 km [DYD+08]. In 2017, Toshiba claims that they achieves 13.7 Mbit/s for 10 km which is shown in QCrypt 2017. Commercially, CLAVIS3 made by ID Quantique achieves 3 kbit/s for 50 km [IDQ15].

Decoy-MDI. The simulation of key rate of decoy-MDI protocol can be found in [ZYW16]. On experimental side, both two implementation [LCW+13, TLX+14] that reported by Lo's survey paper [XCQL15] have combined decoy and MDI protocol. However, their finite key rates are low (< 1 bit/s). Later, Yin *et al.* [YCY+16] demostrated decoy-MDI QKD with much higher key rate. In particular, they achieve the key rate of 321 bit/s for 102 km, 9.55 bit/s for 207 km, 3.2×10^{-4} bit/s for 404 km.

Satellite. The protocol and some commercial progress of satellite QKD can be found in [BAL17]. It was reported [LCL+17] that Micius satellite achieves key rate of 1.1 kbit/s by decoy protocol. Micius satellite also deliver entangled photons over 1200km which two-entangled-photons achieves the rate of 1.1 Hz [YCL+17].

References

[ABB+14] Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Langer, Norbert Lutkenhaus, Christian Monyk, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science, 560 (2014), pp. 62-81*, 2014.

[BAL17] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1), aug 2017.

[BHM96] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651–2658, oct 1996.

[DYD+08] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Optics Express*, 16(23):18790, oct 2008.

[GLLP04] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. 2004.

[HIGM95] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863–1869, mar 1995.

[Hwa03] W. Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. 2003.

[IDQ15] Clavis3 v1.0 specification. Technical report, ID Quantique, 2015.

[ILM07] Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers. Unconditional security of practical quantum key distribution. *European Physical Journal D, Vol 41, p.599*, 2007.

[IWY02] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Physical Review Letters*, 89(3), jun 2002.

[Koa06] Masato Koashi. Unconditional security of quantum key distribution and the uncertainty principle. *Journal of Physics: Conference Series*, 36:98–102, apr 2006.

[Koa09] Masato Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics, Volume 11*, 2009.

[KRS09] Robert Koenig, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Th., vol. 55, no. 9*, 2009.

[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. 1999.

[LCL+17] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, aug 2017.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *PhysRevLett*, 2012.

[LCW+13] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 111(13), sep 2013.

[LJ02] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, jul 2002.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. 2005.

[Lo01] Hoi-Kwong Lo. Proof of unconditional security of six-state quantum key distribution scheme. 2001.

[LS17] Daan Leermakers and Boris Skoric. Security proof for round robin differential phase shift qkd. 2017.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics 4, 686 - 689*, 2010.

[May96] Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channels. 1996.

[MH05] Vadim Makarov and Dag R. Hjelme. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 52(5):691–705, mar 2005.

[MQZL05] X. Ma, B. Qi, Y. Zhao, and H. K. Lo. Practical decoy state for quantum key distribution. 2005.

[MY98] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. 1998.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 2000.

[QFLM07] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation, vol. 7, pp. 073-082*, 2007.

[Ren05] Renato Renner. Security of quantum key distribution. *PhD thesis, ETH Zurich*, 2005.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. 2009.

[SK17] Toshihiko Sasaki and Masato Koashi. A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance. *Quantum Science and Technology*, 2(2):024006, may 2017.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. 2000.

[SYK14] Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475–478, may 2014.

[TKK12] Kiyoshi Tamaki, Masato Koashi, and Go Kato. Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization. 2012.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 2017.

[TLX+14] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters*, 112(19), may 2014.

[TSTK15] Hiroki Takesue, Toshihiko Sasaki, Kiyoshi Tamaki, and Masato Koashi. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photonics*, 9(12):827–831, sep 2015.

[VMH01] Artem Vakhitov, Vadim Makarov, and Dag R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038, nov 2001.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. 2014.

[WTY09] Kai Wen, Kiyoshi Tamaki, and Yoshihisa Yamamoto. Unconditional security of single-photon differential phase shift quantum key distribution. *Physical Review Letters*, 103(17), oct 2009.

[XCQL15] Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Measurement-device-independent quantum cryptography. *EEE JSTQE, Vol.21, No.3, Article:6601111*, 2015.

[YCL+17] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, jun 2017.

[YCY+16] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19), nov 2016.

[ZFQ+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Physical Review A, 78, 042333*, 2008.

[ZYW16] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A*, 93(4), apr 2016.